Attorney Docket No.: BHT-3212-46

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	:	
Donald YANG et al.	:	Group Art Unit: Not Yet Assigned
Application No.: Not Yet Assigned	:	Examiner: Not Yet Assigned
Filed: October 22, 2003	:	

For: **DIGITAL INFORMATION PROTECTING METHOD AND SYSTEM**

CLAIM TO PRIORITY UNDER 35 U.S.C. § 119

Assistant Commissioner of Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

Pursuant to the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55, Applicant claims the right of priority based upon **Chinese Application No. 091124992 filed October 25, 2002.**

A certified copy of Applicant's priority document is submitted herewith.

Respectfully submitted,

By: _____
Bruce H. Troxell
Reg. No. 26,592

TROXELL LAW OFFICE PLLC
5205 Leesburg Pike, Suite 1404
Falls Church, Virginia 22041
Telephone: (703) 575-2711
Telefax: (703) 575-2707

Date: October 22, 2003

中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder：

申　　請　　日 ： 西元 2002 年 10 月 25 日
Application Date

申　請　案　號 ： 091124992
Application No.

申　　請　　人 ： 優碩資訊科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期： 西元 2002 年 12 月 9 日
Issue Date

發文字號： 09111023995
Serial No.

申請日期：91.10.25	案號：91124992
類別：	

（以上各欄由本局填註）

發明專利說明書

一、發明名稱	中文	數位資訊保全方法與系統
	英文	DIGITAL INFORMATION PROTECTING METHOD AND SYSTEM
二、發明人	姓名（中文）	1. 楊大廣 2. 李信達
	姓名（英文）	1. Donald Yang 2. Jim Lee
	國籍	1. 中華民國 2. 中華民國
	住、居所	1. 臺北市士林區克強路10巷3弄2號 2. 台北縣三重市五谷王南街2號
三、申請人	姓名（名稱）（中文）	1. 優碩資訊科技股份有限公司
	姓名（名稱）（英文）	1. Neovue Inc.
	國籍	1. 中華民國
	住、居所（事務所）	1. 台北市忠孝西路一段100號8F
	代表人姓名（中文）	1. 戴英杰
	代表人姓名（英文）	1. Injay W. Tai

四、中文發明摘要　（發明之名稱：數位資訊保全方法與系統）

本發明係一種數位資訊資訊保全方法，係分別於著作端電腦和使用端電腦進行操作。著作端電腦與使用端電腦皆包含一預定之資訊處理軟體，以對一數位資訊進行必要之資訊處理。於該著作端電腦：接收由一伺服器傳送來之一內容金鑰（content key），並以該內容金鑰對該數位資訊進行加密；接著以一預定之金鑰加密程序對該內容金鑰進行加密；並將加密後的數位資訊與加密後的內容金鑰一起傳送至該使用端電腦。於該使用端電腦：以相對應之預定的金鑰解密程序對該內容金鑰進行解密；以該內容金鑰對所接收到的加密數位資訊進行解密，以便於該使用端電腦可對該數位資訊進行閱覽。由於本發明將數位資訊內容與內容金鑰分別進行加密並一起傳送至使用端，藉此，

英文發明摘要　（發明之名稱：DIGITAL INFORMATION PROTECTING METHOD AND SYSTEM）

The present invention is a digital information protecting method executed in an auther computer and a client computer respectively. Both the auther computer and the client computer has a predetermined information processing software to process a piece of information. In the auther computer: first, receives a content key from a server and encrypts the piece of information by the content key; second, encrypts the content key by a predetermined key encrypting process; third,

四、中文發明摘要　（發明之名稱：數位資訊保全方法與系統）

本發明可使得數位資訊受到更嚴密的保護，且不論使用者在連線至網路（on-line）或是離線（off-line）的狀態下，皆可擷取解密所需的金鑰，再由使用端電腦解密數位資訊，以供使用者進行閱覽。

英文發明摘要　（發明之名稱：DIGITAL INFORMATION PROTECTING METHOD AND SYSTEM）

transismits the encrypted information and encrypted content key to the client computer. In the client computer: first, decrypts the encrypted content key by a corresponding predetermined decrypting process; second, decrypts the encrypted information by the content key to make the piece of information can be used by the client computer. The present invention encrypts the piece of information and the content key respectively, and transimits both encrypted information and

四、中文發明摘要　（發明之名稱：數位資訊保全方法與系統）

英文發明摘要　（發明之名稱：DIGITAL INFORMATION PROTECTING METHOD AND SYSTEM）

encrypted content key to the client computer at the same time. So the present invention protects the piece of information strictly. Besides, no matter the client computer is on-line or off-line, the client computer can get the key to descrypt the piece of information to make the piece of information be used by a user.

本案已向

國(地區)申請專利	申請日期	案號	主張優先權
無			

有關微生物已寄存於	寄存日期	寄存號碼
無		

五、發明說明（1）

發明領域

本發明係關於一種數位資訊資訊保全方法與系統；特別是一種經過雙重加密，令數位資訊不論在離線或線上狀態下皆可解密閱覽的方法與系統。

發明背景

隨著網際網路（Internet）的發達，由於簡單的操作介面以及方便的使用環境，網路的使用者往往不知不覺就抄襲了其他人於網路上發表的作品。這些在網路上發表作品（如各式文章、歌曲、各式軟體等）的著作人，有些作品僅是希望藉由網路達到知識快速散佈與推廣的目的，有些作品甚至並非由著作人自己在網路上散播。這些著作人並未料及自己的作品會被其他人加以盜用，因此而喪失了自己應有的權益。這種網路上侵犯著作權的問題已經日益氾濫，為了解決諸如此類的問題，數位權證管理（Digital Rights Management，DRM）的相關技術便應運而生。

所謂的數位權證管理，主要是用來管制數位資訊在網路上的非法散佈，其使得僅有獲得著作人授權的使用者，可以依據著作人原先所同意的使用範圍與期限來使用數位資訊，而未獲得授權的使用者則無法使用甚至無法存取數位資訊。此種類型的數位權證管理軟體，較知名的有Authentica PageRecall以及Alchemedia Mirage等。但是，上述的數位權證管理軟體卻仍然可以讓未授權者下載

加密的數位資訊，如果未授權者一旦對加密後的數位資訊成功解密，則數位資訊就如同未受到數位權證管理軟體的保護一般。

為了解決上述的問題，美國專利第6,289,450號以及美國專利第6,339,825號，便提出了設定資訊保密政策（policy）來保護數位資訊不被未授權者存取的方法。

但是上述的各種數位資訊的保護方法仍有兩個缺點。其一，當數位權證軟體在對數位資訊進行加密時，僅是利用簡單的單層加密方式，而且將解密的金鑰就放在加密後的數位資訊中。因此，習知技藝者有可能可以利用各種方式找出解密金鑰的位置，而將加密後的數位資訊進行解密。其二，如果數位資訊中未附加解密金鑰，使用者要使用或閱覽數位資訊，就必須要連線上網路以便線上即時取得解密所需的金鑰。如此一來，當使用者所處的時空環境不方便上網時，就無法閱覽數位資訊，連帶使得數位資訊的使用便利性大打折扣。

因此，必須提出一種新的數位權證管理方案來解決上述問題。

發明概述

本發明之一目的在於提供一種利用雙重加/解密來對數位資訊進行更深一層保護的方法。即除了習知技術的單層加密之外，另外針對原先用以加密的金鑰進行加密後再附加於數位資訊中，因此可以使得數位資訊受到更嚴密的

保護。

本發明之另一目的在於提供一種可離線預覽的數位資訊保護方法。本發明之加解密的金鑰皆放置在電腦或是資訊處理裝置中的軟體或直接就附加在數位資訊中，不需連線至網路下載解密所需的金鑰，即可進行解密程序。因此可令使用者在離線狀態下使用數位資訊，提高了數位資訊的便利性，又因有金鑰加/解密程序對於內容金鑰的多一層保護，也不至於因便利性而喪失了保密性。

本發明係一種數位資訊資訊保全方法，用以在一伺服器之協助下，將一著作端電腦(author computer)之數位資訊(a piece of information)加密後經由一電腦網路傳送至一使用端電腦(client computer)解密以進行閱覽。其中，著作端電腦與使用端電腦皆包含一預定之資訊處理軟體，以對數位資訊進行必要之資訊處理。

本發明之數位資訊保全方法包含下列步驟：

（於著作端電腦）

接收由伺服器傳送來之一內容金鑰（content key），並以內容金鑰對數位資訊進行加密。接著以一預定之金鑰加密程序對內容金鑰進行加密，並將加密後的數位資訊與加密後的內容金鑰一起傳送至使用端電腦。

（於使用端電腦）

以相對應金鑰加密程序之預定的金鑰解密程序對內容金鑰進行解密。以內容金鑰對所接收到的加密數位資訊進行解密，以便於使用端電腦可對數位資訊進行閱覽。

關於本發明之優點與精神可以藉由以下的發明詳述及所附圖式得到進一步的瞭解。

發明之詳細說明

請參閱圖一，圖一係為本發明第一較佳具體實施例之示意圖。本發明所述之數位資訊保全系統，係建構在一伺服器10、一著作端電腦12以及一使用端電腦14之間。此處所謂數位資訊15，則可以泛指電子文件、電子郵件、數位圖片、動畫等。如圖一所示，數位資訊15傳遞的過程如下：首先，由著作人16在著作端電腦12上著作完成數位資訊15後，透過伺服器所提供的一第一資訊處理軟體來訂定一資訊保密政策120，之後並透過網際網路，將資訊保密政策120傳送到伺服器10中。所謂的資訊保密政策120，即是著作人16對其所著作之數位資訊15設立的使用規定，這些規定可能包括授權的內容範圍、授權的時間、授權的使用次數以及對數位資訊15進行儲存、複製、轉貼或列印的限制等。

伺服器10在本發明第一較佳具體實施例中乃扮演一輔助的角色，其用以提供數位資訊處理軟體于著作端電腦12與使用端電腦14使用，以及當接收到由著作端電腦12傳回的資訊保密政策120，便提供可對數位資訊10的內容進行加密的一內容金鑰110給著作端電腦12。

如果一使用者18在使用端電腦14想要使用數位資訊15，其首先須由伺服器10、著作端電腦12或任何提供該資

訊處理軟體處下載一第二資訊處理軟體，並必須獲得著作人16的授權才可使用數位資訊15，且授權的範圍依資訊保密政策120而定。當使用者18獲得授權後，便可以下載數位資訊15。待下載數位資訊15後，便可透過第二資訊處理軟體對數位資訊15解密後並加以使用。在此特別強調一點，本發明較佳具體實施例中的資訊處理軟體係以AES(Advanced Encryption Standard)方法對數位資訊15進行加/解密，由於AES方法可以支援128位元，甚至是高達256位元的加解密，是目前公認最安全的加解密演算法之一。此外，本發明所有的加解密方法採取的是對稱型加解密方法，因此，加密時所使用的金鑰與解密時所使用的金鑰是同一把金鑰。至於儲存在著作端電腦或是使用端電腦中的第一與第二資訊處理軟體，在本發明之較佳實施例中是同一套軟體的不同備份，其中的軟體模組與金鑰是完全相同，只是基於安裝於不同電腦中，給予不同標號以資識別。

請參照圖二，圖二係圖一中著作端電腦12的操作示意圖。著作端電腦12的應用方式，主要是憑藉著由伺服器10所下載的一第一資訊處理軟體20為操作平台，來對其著作的數位資訊15進行保護。在著作端電腦12中的第一資訊處理軟體20包含一內容加密模組22、一金鑰加密模組24、複數個編有序號的通用金鑰（Universal Key）UK_i以及。首先，當數位資訊15被著作完成時，著作人16會在第一資訊處理軟體20所提供的介面下，對數位資訊15設定資訊保密

政策120，來規範關於數位資訊15存取及使用的規定，其中可能包含一離線使用許可，來允許使用者可以在離線的狀態下讀取數位資訊15。一般而言，一旦取得離線使用許可，表示使用者對於數位資訊的使用情形會脫離著作人與伺服器的掌控。因此，為了加強對於數位資訊的保障，在這種可離線使用的情形下，一般會讓使用者對於其手上數位資訊的使用自由度降低，限制會較多。例如，只能在電腦的螢幕上閱覽，而不能進行其他如轉存、列印等的功能。

當著作人16完成資訊保密政策120後，第一資訊處理軟體20會將資訊保密政策120傳送至伺服器10，伺服器10則在收到資訊保密政策120後，傳送一內容金鑰（Content Key）110至著作端電腦18。

第一資訊處理軟體20中的內容加密模組22則在資訊保密政策120設定後，會由伺服器10下載一內容金鑰110，並根據內容金鑰110對數位資訊15進行加密。金鑰加密模組24則是當數位資訊15以內容金鑰110加密完成後，根據一金鑰加密程序再對內容金鑰110進行加密。

請參閱圖三，圖三係圖二中經過雙重加密後的數位資訊40示意圖。所謂的金鑰加密程序，係本發明對內容金鑰110以及被內容金鑰110加密的數位資訊48所建立的一道更嚴謹的防線。首先，金鑰加密模組24需從內建於第一資訊處理軟體20中的複數個通用金鑰UK_i中選擇其一，以對內容金鑰110進行加密，其中每一個通用金鑰UK_i都有其相對

應的序號以茲識別。金鑰加密模組24再將加密後的內容金鑰42、通用金鑰所對應之序號44以及資訊保密政策120儲存至一標頭檔(header)46中，並附加於經過內容加密的數位資訊48之前。其中，資訊保密政策120乃視情況所需，全部或部分附加於標頭檔46中。

請參照圖四，圖四係本發明金鑰加密程序之流程圖。本發明所應用之雙重加密程序，即是在習知僅有單層的內容加密之外，再添加一道加密過程。其包含下列步驟：

步驟S30：接收內容金鑰42，接著進行步驟S31。

步驟S31：利用內容金鑰42對數位資訊進行加密，以產生加密後的數位資訊40，接著進行步驟S32。

步驟S32：選擇一通用金鑰UK_i，接著進行步驟S32。

步驟S33：根據通用金鑰UK_i對內容金鑰110進行加密，接著進行步驟S34。

步驟S34：將所選擇通用金鑰UK_i相對應的序號44、被加密後的內容金鑰42以及資訊保密政策120共同儲存在一標頭檔46中，接著進行步驟S36。

步驟S36：將標頭檔46附加於加密後的數位資訊48之前。

至此，即完成了本發明之金鑰加密程序。著作端電腦12則在完成了數位資訊15的雙重加密過程後，會以數位傳播的方式，將此雙重加密後的數位資訊40散播出去。數位傳播的方式則以使用者18可以收到雙重加密後的數位資訊40為原則即可，不論是傳統用磁片、光碟片等資訊載體，

或是以企業內部網路、外部網路、網際網路等傳送電子郵件的方式都可以。

請參照圖五，圖五係圖一中使用端電腦14的操作示意圖。如果一使用者18想要使用著作端電腦12所雙重加密的數位資訊40，其必須先獲得授權，始有資格下載數位資訊40。但除了獲得著作端電腦12的授權外，使用端電腦14必須下載一第二資訊處理軟體50，才能對數位資訊40進行處理。本發明之第二資訊處理軟體50之中包含了一金鑰解密模組52和一內容解密模組54。

第二資訊處理軟體50的操作方式，首先是由金鑰解密模組52以一金鑰解密程序對其接收到的數位資訊40進行解密的動作。請參閱圖六，圖六係圖五中經過金鑰解密後的數位資訊15示意圖。所謂的金鑰解密程式，係由第二資訊處理軟體50在接收到雙重加密後的數位資訊40後，先由標頭檔46中記載的序號，找出第二資訊處理軟體中相對應序號44的通用金鑰UK_i，並以通用金鑰UK_i對加密後的內容金鑰42進行解密。經由雙重解密程序之後，該內容解密模組54會獲得內容金鑰110，並以內容金鑰110對加密後的數位資訊48進行解密，而可以閱覽數位資訊15。

在此特別強調一點，由於本發明第一較佳具體實施例的各種解密金鑰皆是放置於獲得授權的使用端電腦14中，因此如果使用者18想要離線使用數位資訊時，可以要求著作端電腦12發給一離線使用許可。此離線使用許可通常會有最嚴格的限定，來明確規範其使用的範圍以及次數，以

免數位資訊遭到其他人的盜用。請參照圖七，圖七係本發明雙重解密程序之流程圖。本發明之雙重解密程序係透過使用端電腦14中的第二資訊處理軟體50加以執行。

步驟S60：接收雙重加密後的數位資訊40，接著進行步驟S62。

步驟S64：根據標頭檔46中所記載的序號44，從第二資訊處理軟體中找出相對應的通用金鑰UK_i，接著進行步驟S66。

步驟S66：根據此通用金鑰UK_i對該標頭檔46中加密的內容金鑰42進行解密，接著進行步驟S68。

步驟S68：獲得解密後的內容金鑰110。

請參閱圖八，圖八係本發明第二具體實施例之示意圖。本發明第二具體實施例與第一具體實施例最大的不同之處，在於使用端電腦14所下載的第三資訊處理軟體60中，並未包含複數個通用金鑰UK_i。因此需在收到加密後的數位資訊40後，透過資訊保密政策中的規定，自伺服器10中下載解密內容金鑰用的通用金鑰UK_i。待使用端電腦14中的第三資訊處理軟體60獲得通用金鑰UK_i，後續的解密動作則和第一具體實施例中的相當。

伺服器10在本發明第二較佳具體實施例中乃扮演一主動輔助的角色，其用以提供數位資訊處理軟體于著作端電腦12與使用端電腦14使用，以及當接收到由著作端電腦12傳回的資訊保密政策120，便提供可對數位資訊10的內容進行加密的一內容金鑰110給著作端電腦12，並根據資訊

保密政策120的規定，提供通用金鑰給使用端電腦14中的第三資訊處理軟體60使用，以進行後續的解密動作。

接下來將綜合以上所述，對本發明數位資訊的保全方法及系統作一完整的流程介紹。請參閱圖九，圖九係本發明之數位資訊保全方法的流程圖。本發明保護數位資訊的方法包含：

步驟S70：開始，著作人16於著作端電腦18上完成數位資訊15，接著進行步驟S71。

步驟S71：著作人16於第一資訊處理軟體20中設定關於數位資訊15的資訊保密政策120，接著進行步驟S72。

步驟S72：傳送資訊保密政策120至伺服器10，接著執行步驟S73。

步驟S73：伺服器10處傳送內容金鑰110至著作端電腦12，接著進行步驟S74。

步驟S74：第一資訊處理軟體20以內容金鑰110對數位資訊15進行加密，接著進行步驟S75。

步驟S75：第一資訊處理軟體20自複數個通用金鑰UK_i中選擇其一，接著進行步驟S76。

步驟S76：第一資訊處理軟體20以選到的通用金鑰UK_i對內容金鑰110進行加密，接著進行步驟S77。

步驟S77：第一資訊處理軟體20將加密後的內容金鑰42與通用金鑰UK_i所對應之序號以及必要的資訊保密政策120儲存至一標頭檔46中，接著進行步驟S78。

步驟S78：第一資訊處理軟體20將標頭檔46附加於經

過加密的數位資訊48之前，接著進行步驟S79。

步驟S79：將雙重加密後的數位資訊40傳送至使用端電腦12，接著進行步驟S791。

步驟S80：使用端電腦獲得伺服器授權並下載第二資訊處理軟體，接著進行步驟S81。

步驟S81：檢查解密後的標頭檔46中是否存有該著著作人16所授權之離線存取許可，若是，則可在離線狀態下進行步驟S82；若否，則以連線的方式進行步驟S82。

步驟S82：依據標頭檔46中所儲存的序號擷取相對應之通用金鑰UK_i，接著進行步驟S83。

步驟S83：以通用金鑰UK_i對經過加密的內容金鑰42進行解密，接著進行步驟S84。

步驟S84：以解密後的內容金鑰110對加密後的數位資訊48進行解密，接著進行步驟S85。

步驟S85：使用端電腦12可對數位資訊15進行閱覽。

本發明的優點可歸納如下：

1. 除了一般以內容金鑰對於數位資訊進行加密的普遍作法，本發明還利用通用金鑰對內容金鑰進行加密，解密時反之進行；這種不僅對於所欲保護的數位資訊進行保護，且對於內容金鑰也進行保護的雙重加/解密技術，較習知單層加密技術更有效的保護數位資訊。

2. 將用來加密數位資訊的內容金鑰附加於加密後的數位資訊中，因此只要使用者通過資訊保密政策，甚至可在很多離線的情況下瀏覽數位資訊的內容，提高了使用者對

於數位資訊的可利用性。

3. 資訊處理軟體中的複數個通用金鑰是編譯(compile)於資訊處理軟體中，除非可以完整破解整個資訊處理軟體，否則通用金鑰被取得的機會極低。

4. 欲破解本發明所欲保護的數位資訊，必須取得內容金鑰，但是內容金鑰是經過加密並隨附於加密後的數位資訊傳送出去，而對內容金鑰解密則必須依賴通用金鑰的序號以及通用金鑰本身，因此本發明設計將通用金鑰編譯放置於資訊處理軟體中，如此一來，完整的加/解密程序所需的訊息分置於數位資訊檔案與資訊處理軟體中，因而分散了數位資訊被破解的風險，相形之下提高了數位資訊的安全性。

藉由以上較佳具體實施例之詳述，係希望能更加清楚描述本發明之特徵與精神，而並非以上述所揭露的較佳具體實施例來對本發明之範疇加以限制。相反地，其目的是希望能涵蓋各種改變及具相等性的安排於本發明所欲申請之專利範圍的範疇內。因此，本發明所申請之專利範圍的範疇應該根據上述的說明作最寬廣的解釋，以致使其涵蓋所有可能的改變以及具相等性的安排。

圖式之簡易說明

圖一係本發明第一較佳具體實施例之示意圖。

圖二係圖一中著作端電腦的操作示意圖。

圖三係圖二中經過雙重加密後的數位資訊示意圖。

圖四係本發明金鑰加密程序之流程圖。

圖五係圖一中使用端電腦的操作示意圖。

圖六係圖五中經過雙重解密後的數位資訊示意圖。

圖七係本發明金鑰解密程序之流程圖。

圖八係本發明第二較佳具體實施例之示意圖。

圖九係本發明之數位資訊保全方法的流程圖。

圖式之標號說明

10：伺服器　　12：著作端電腦

14：使用端電腦　　16：著作人

18：使用者　　110：內容金鑰

120：資訊保密政策　　20：第一資訊處理軟體

22：內容加密模組　　24：金鑰加密模組

UK_i：通用金鑰　　40：雙重加密後的數位資訊

42：加密後的內容金鑰　　44：序號

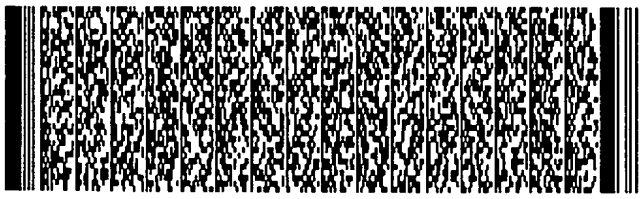
46：標頭檔　　47：加密後的標頭檔

48：加密後的數位資訊　　50：第二資訊處理軟體

52：金鑰解密模組　　54：內容解密模組

60：第三資訊處理軟體

S30~S38：雙重加密程序之步驟



圖式簡單說明

S60~S68：雙重解密程序之步驟

S70~S85：數位資訊保全方法之步驟

六、申請專利範圍

1、一種數位資訊保全方法，以在一伺服器之協助下，將一著作端電腦(author computer)之一數位資訊(a piece of information)加密後經由一電腦網路傳送至一使用端電腦(client computer)解密以進行閱覽，該著作端電腦與該使用端電腦皆包含一預定之資訊處理軟體，以對該數位資訊進行必要之資訊處理，該方法包含：

於該著作端電腦：

接收由該伺服器傳送來之一內容金鑰（content key），並以該內容金鑰對該數位資訊進行加密；

以一預定之金鑰加密程序對該內容金鑰進行加密；以及

將該加密後的數位資訊與該加密後的內容金鑰一起傳送至該使用端電腦；

於該使用端電腦：

以相對應該金鑰加密程序之預定的一金鑰解密程序對該加密後的內容金鑰進行解密；以及

以該內容金鑰對所接收到的該加密後的數位資訊進行解密，以便於該使用端電腦可對該數位資訊進行閱覽。

2、如申請專利範圍第1項所述之資訊保全方法，其中該著作端電腦並制定與該數位資訊相關之一資訊保密政策（policy），且將其傳送至該伺服器。

3、如申請專利範圍第2項所述之資訊保全方法，其中該

資訊保密政策係包含該資訊授權的範圍、時間以及閱讀次數等規定。

4、如申請專利範圍第1項所述之資訊保全方法，其中該著作端電腦之資訊處理軟體包含複數個編有序號之通用金鑰。

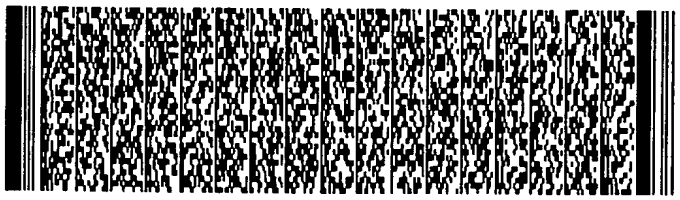
5、如申請專利範圍第4項所述之資訊保全方法，其中該金鑰加密程序係由該著作端電腦之資訊處理軟體執行下列步驟：

自該複數個通用金鑰中選擇其一，並以選擇的該通用金鑰對該內容金鑰進行加密；以及

將該加密後的內容金鑰與該通用金鑰所對應之序號儲存至一標頭檔(header)中，並附加於該經過加密的數位資訊之前。

6、如申請專利範圍第5項所述之資訊保全方法，其中該著作端電腦之資訊處理軟體執行該金鑰加密程序之前，會請求該著作端電腦之著作者授權一離線存取許可(Off-line Access Permission)。

7、如申請專利範圍第6項所述之資訊保全方法，其中該離線存取許可決定該使用端電腦是否可於離線的狀態，對所接收到的數位資訊進行處理與閱覽。



8、 如申請專利範圍第7項所述之資訊保全方法，其中該金鑰解密程序係由該使用端電腦之資訊處理軟體執行下列步驟：

根據該標頭檔中所儲存之序號擷取出相對應的該通用金鑰；以及

以該通用金鑰對該內容金鑰進行解密。

9、 如申請專利範圍第8項所述之資訊保全方法，其中該使用端電腦之資訊處理軟體係根據該序號自該伺服器下載該通用金鑰

10、如申請專利範圍第8項所述之資訊保全方法，其中該使用端電腦之資訊處理軟體係包含該複數個通用金鑰，該使用端電腦之資訊處理軟體係利用該序號選取相對應之通用金鑰。。

11、如申請專利範圍第1項所述之資訊保全方法，其中該資訊處理軟體係以AES(Advanced Encryption Standard)方法進行加/解密。

12、一種數位資訊保全系統，以在一伺服器之監督下，將一著作端電腦(author computer)之數位資訊(a piece of information)加密後經由一電腦網路傳送至一使用端電腦

六、申請專利範圍

(client computer)解密以進行閱覽，該著作端電腦與該使用端電腦皆包含一預定之資訊處理軟體，以對該數位資訊進行必要之資訊處理，該系統包含：

一第一資訊處理軟體，係設置於該著作端電腦，包含：

一內容加密模組，用以接收由該伺服器傳送來之一內容金鑰（content key）；以及

利用該內容金鑰對該數位資訊進行加密；以及

一金鑰加密模組，用以利用一預定之金鑰加密程序對該內容金鑰進行加密，並且將加密後的數位資訊與加密後的內容金鑰一起傳送至該使用端電腦；

一第二資訊處理軟體，係設置於該使用端電腦，包含：

一金鑰解密模組，用以利用相對應該雙重加密程序之預定的金鑰解密程序對該內容金鑰進行解密；以及

一內容解密模組，用以利用該內容金鑰對所接收到的加密數位資訊進行解密，以便於該使用端電腦可對該數位資訊進行閱覽。

13、如申請專利範圍第12項所述之資訊保全系統，其中該著作端電腦並制定與該數位資訊相關之一資訊保密政策（policy），且將其傳送至該伺服器。

14、如申請專利範圍第13項所述之資訊保全系統，其中該

六、申請專利範圍

資訊保密政策係包含該資訊授權的範圍、時間以及閱讀次數等規定。

15、如申請專利範圍第12項所述之資訊保全系統，其中該資訊處理軟體包含複數個編有序號之通用金鑰。

16、如申請專利範圍第15項所述之資訊保全系統，其中該金鑰加密程序係由該著作端電腦之資訊處理軟體執行下列步驟：

自該複數個通用金鑰中選擇其一，並以選擇的該通用金鑰對該內容金鑰進行加密；以及

將該加密後的內容金鑰與該通用金鑰所對應之序號儲存至一標頭檔(header)中，並附加於該經過加密的數位資訊之前。

17、如申請專利範圍第16項所述之資訊保全系統，其中該著作端電腦之資訊處理軟體執行該金鑰加密程序之前，會請求該著作端電腦之著作者授權一離線存取許可(Off-line Access Permission)。

18、如申請專利範圍第17項所述之資訊保全系統，其中該離線存取許可決定該使用端電腦是否可於離線的狀態，對所接收到的數位資訊進行處理與閱覽。

六、申請專利範圍

19、如申請專利範圍第18項所述之資訊保全系統，其中該金鑰解密程序係由該使用端電腦之資訊處理軟體執行下列步驟：

根據該標頭檔中所儲存之序號擷取出該通用金鑰；以及

以該加密金鑰對該內容金鑰進行解密。

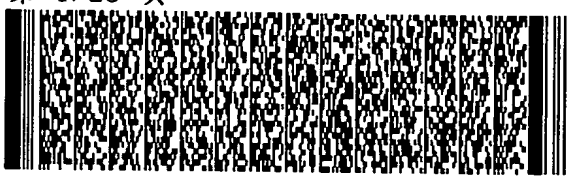
20、如申請專利範圍第19項所述之資訊保全方法，其中該使用端電腦之資訊處理軟體係根據該序號自該伺服器下載該通用金鑰，該使用端電腦之資訊處理軟體係利用該序號選取相對應之通用金鑰。。

21、如申請專利範圍第19項所述之資訊保全方法，其中該使用端電腦之資訊處理軟體係包含該複數個通用金鑰。

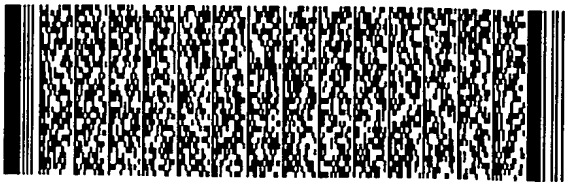
22、如申請專利範圍第12項所述之資訊保全系統，其中該資訊處理軟體係以AES(Advanced Encryption Standard)方法進行加/解密。

申請案件名稱:數位資訊保全方法與系統

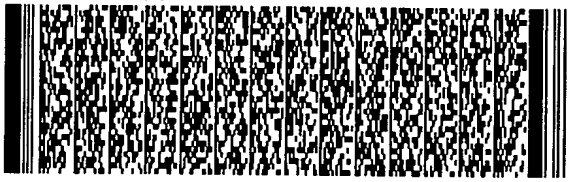
第 1/25 頁



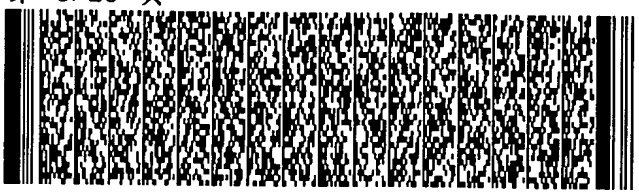
第 2/25 頁



第 2/25 頁

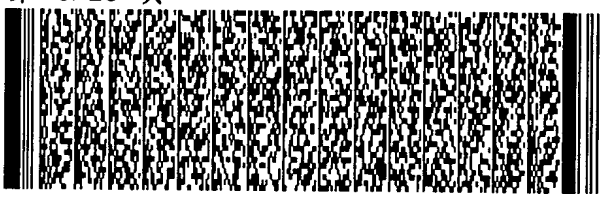


第 3/25 頁

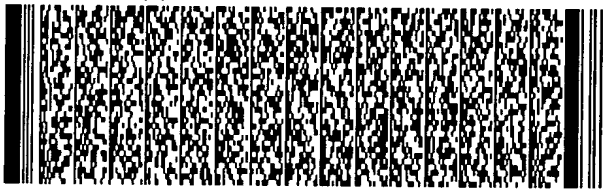


第 4/25 頁

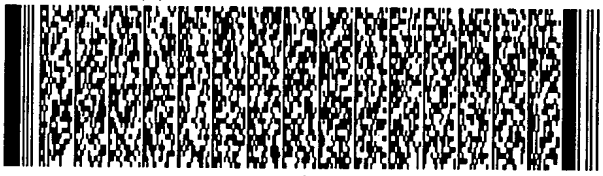
第 6/25 頁



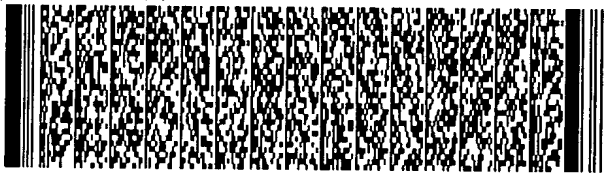
第 6/25 頁



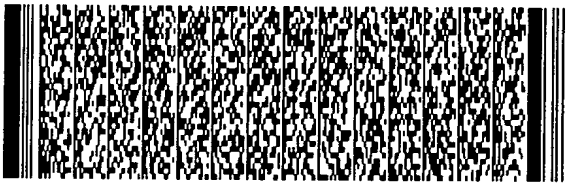
第 7/25 頁



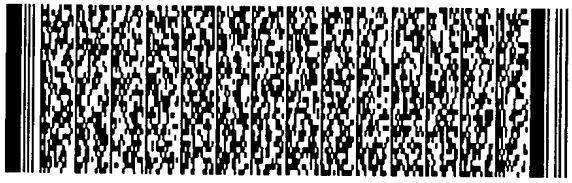
第 7/25 頁



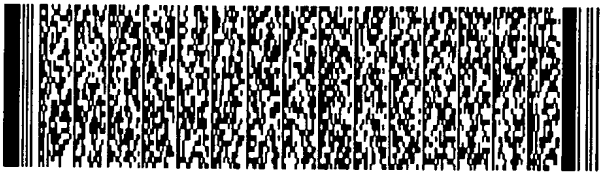
第 8/25 頁



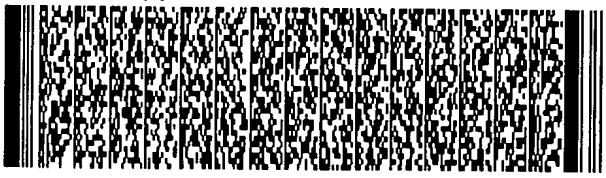
第 8/25 頁



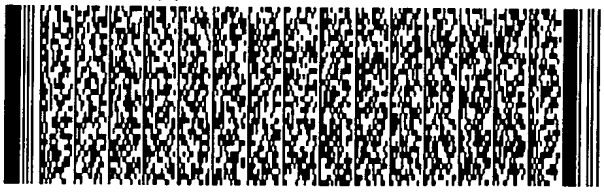
第 9/25 頁



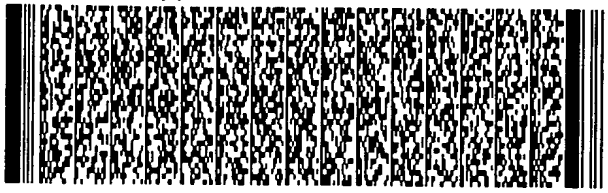
第 9/25 頁



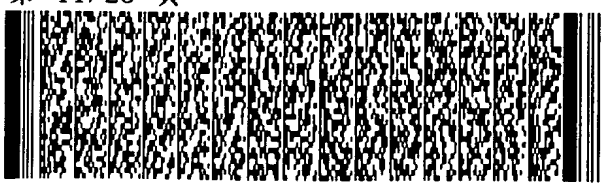
第 10/25 頁



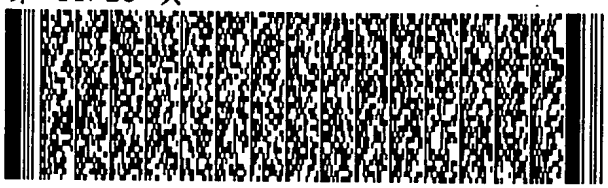
第 10/25 頁



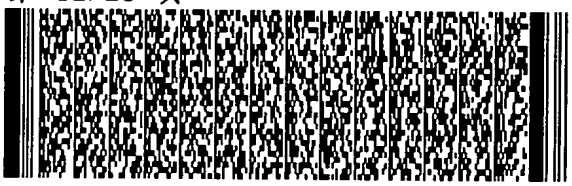
第 11/25 頁



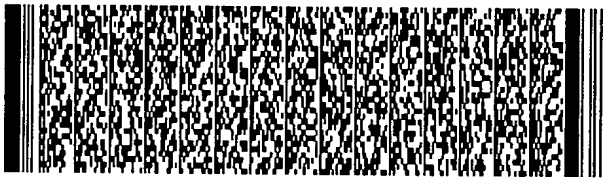
第 11/25 頁



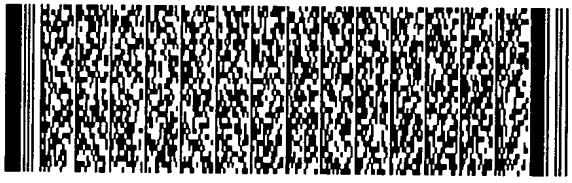
第 12/25 頁



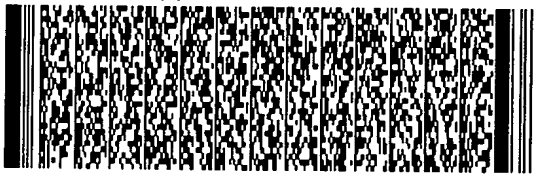
第 13/25 頁



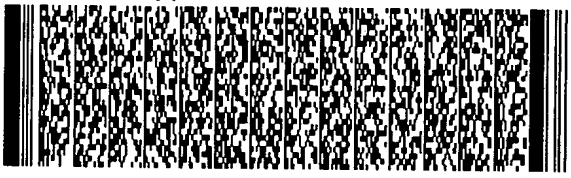
第 14/25 頁



第 15/25 頁



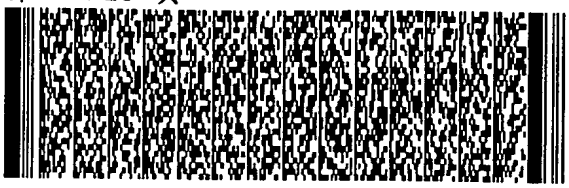
第 16/25 頁



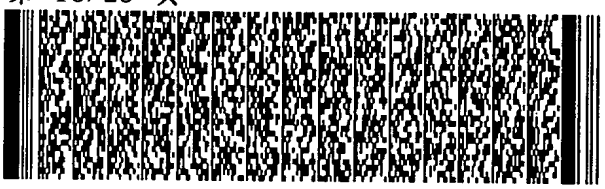
第 17/25 頁

第 19/25 頁

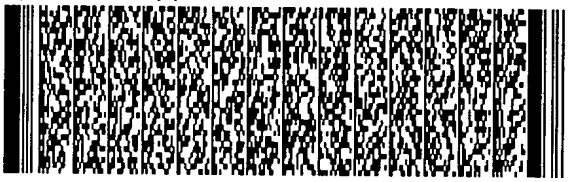
第 12/25 頁



第 13/25 頁

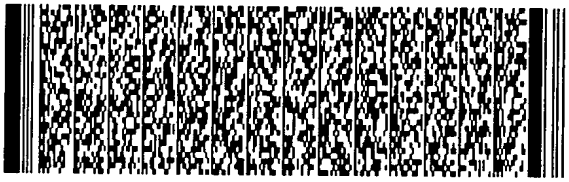


第 14/25 頁

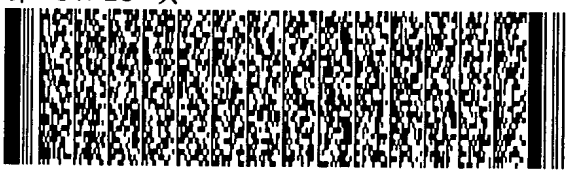


第 15/25 頁

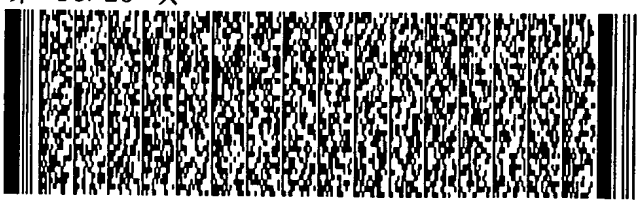
第 16/25 頁



第 17/25 頁

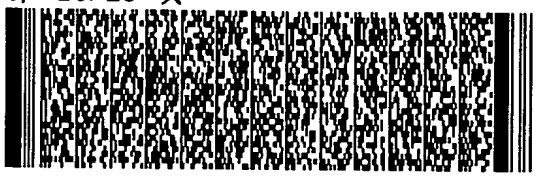


第 18/25 頁

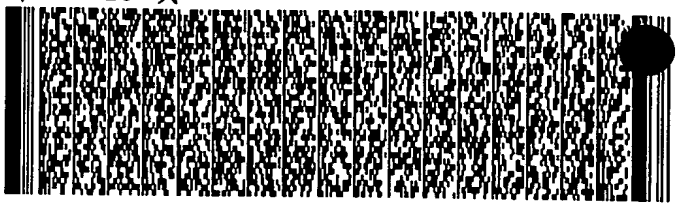


第 20/25 頁

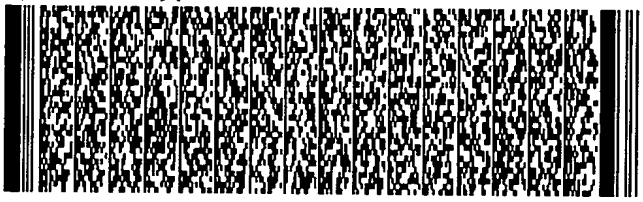
第 20/25 頁



第 21/25 頁



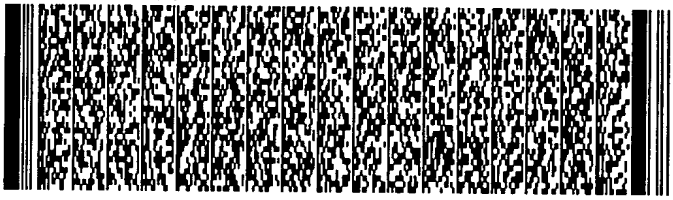
第 22/25 頁



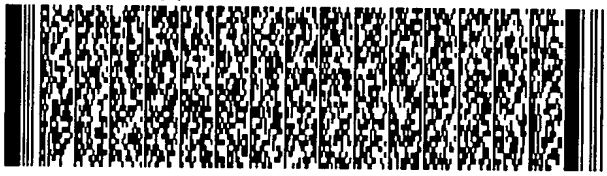
第 23/25 頁

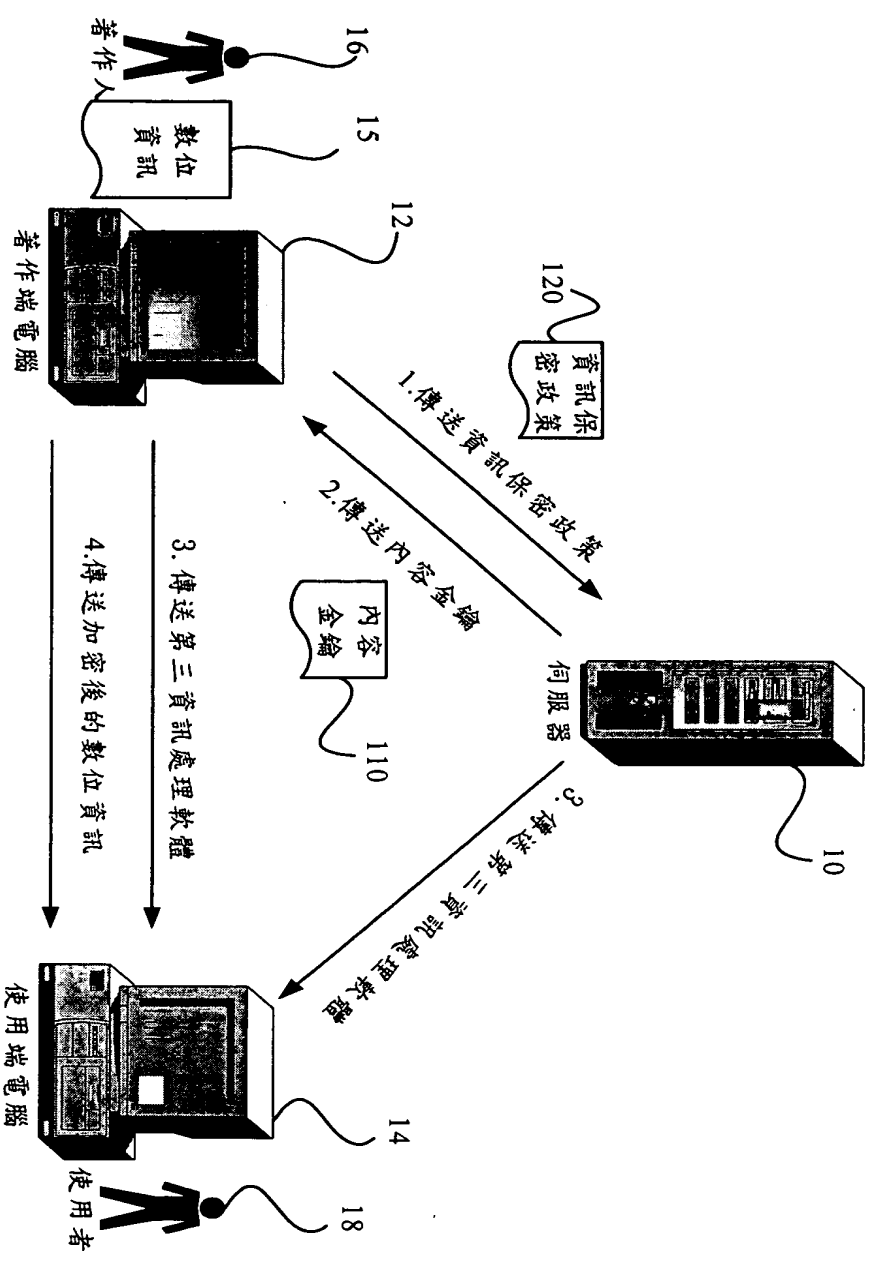
第 23/25 頁

第 24/25 頁



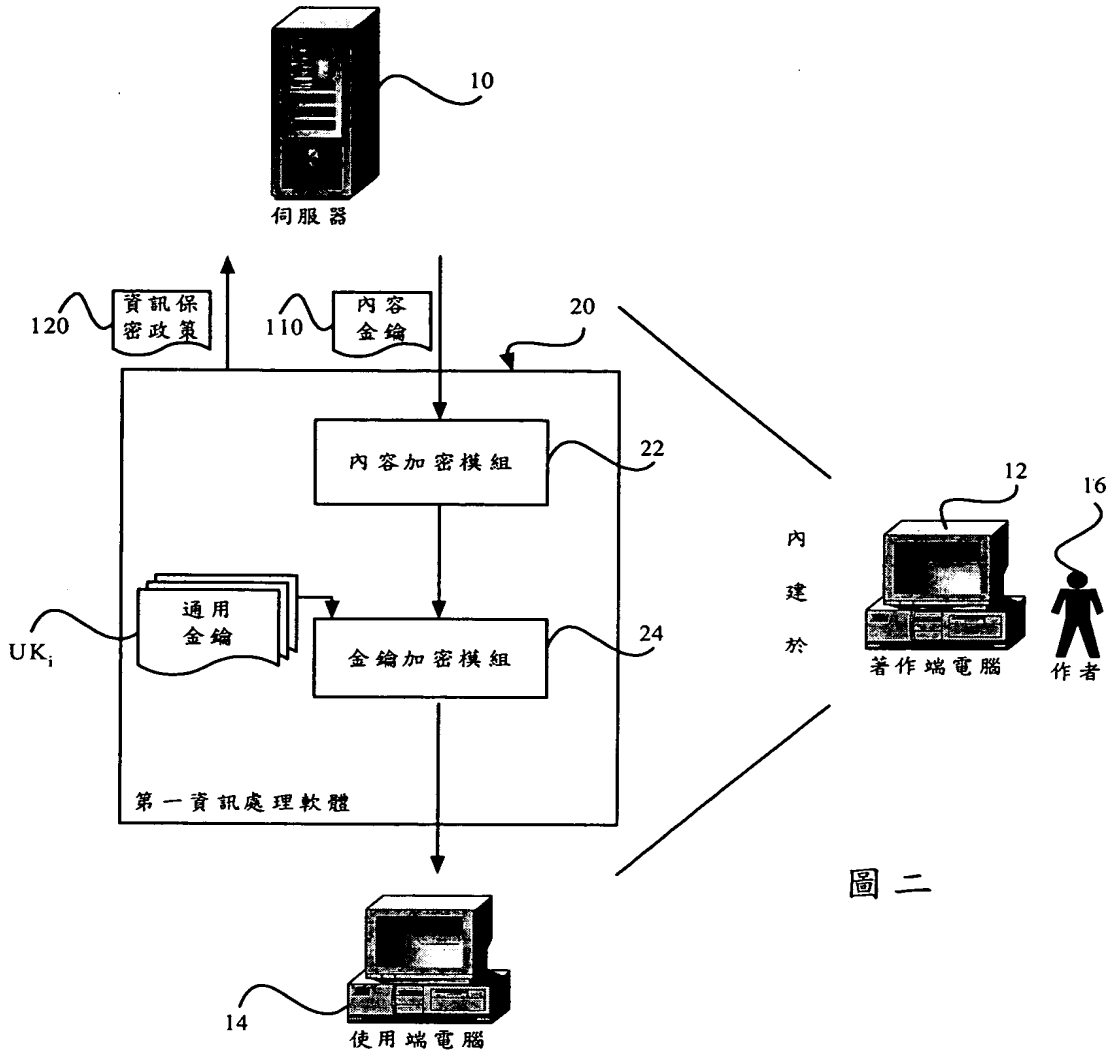
第 25/25 頁




著作人
16
數位資訊
15
12
著作端電腦
資訊保密政策
120
1.傳送資訊保密政策
2.傳送內容金鑰
內容金鑰
110
伺服器
10
3.傳送第三資訊處理軟體
4.傳送加密後的數位資訊
使用端電腦
14
使用者
18

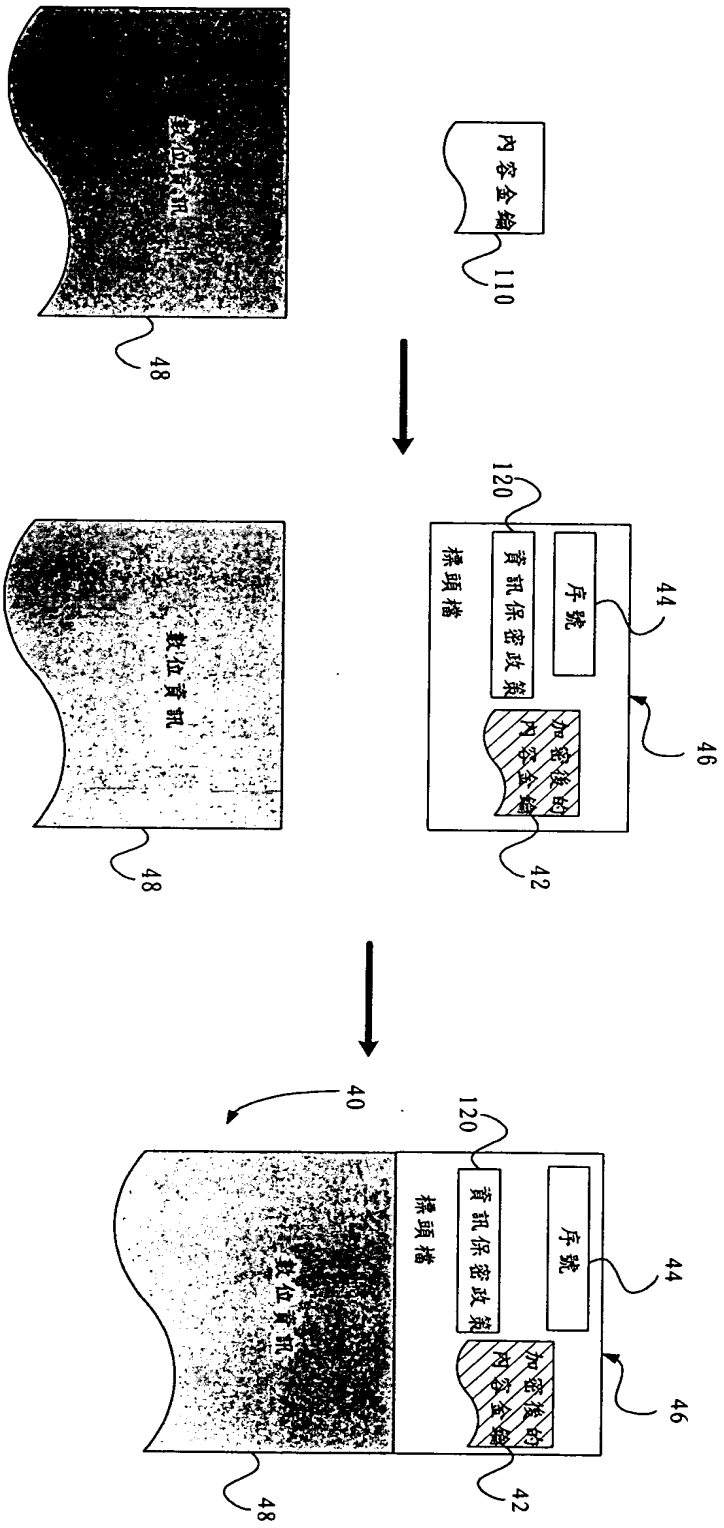
圖一

圖式


10
伺服器
120
資訊保密政策
110
內容金鑰
20
內容加密模組
22
通用金鑰
UK_i
金鑰加密模組
24
第一資訊處理軟體
內建於
12
16
著作端電腦
作者
14
使用端電腦

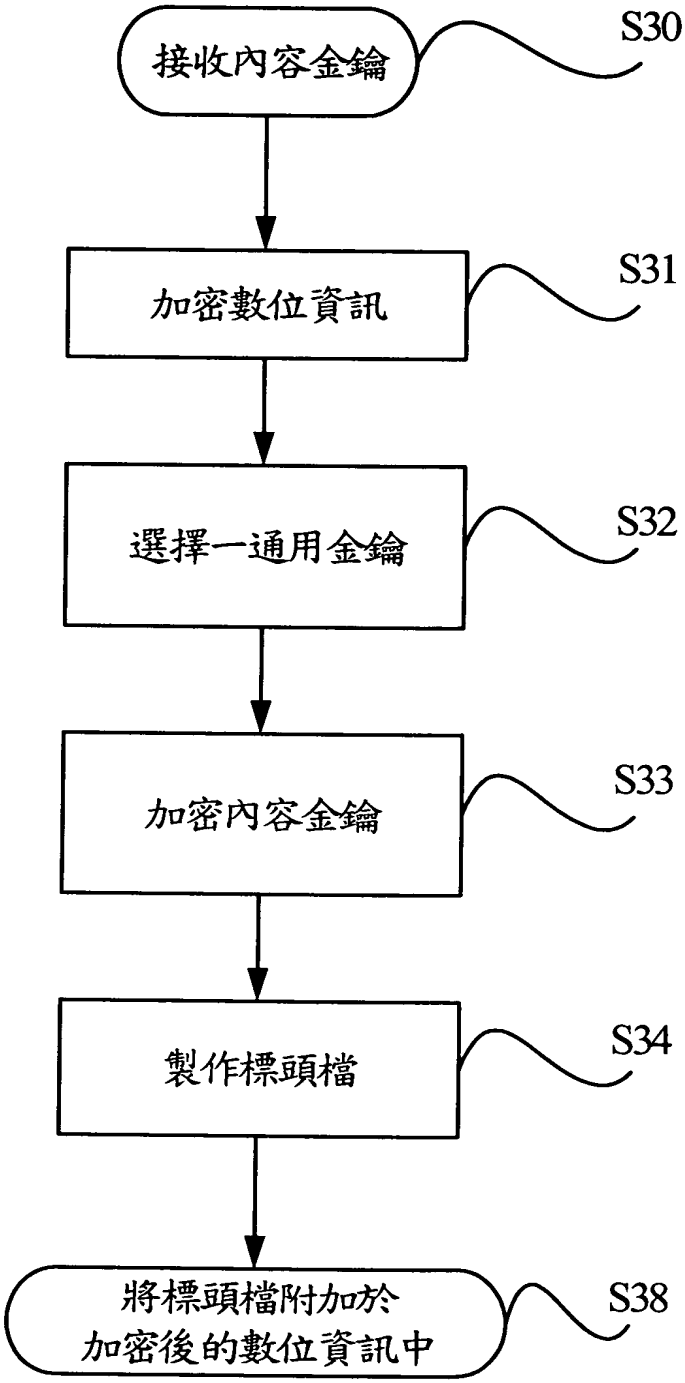
圖二

圖式


內容金鑰
110
數位資訊
48
120
資訊保密政策
序號
44
46
加密後的內容金鑰
42
標頭檔
數位資訊
48
40
120
資訊保密政策
序號
44
46
加密後的內容金鑰
42
標頭檔
數位資訊
48

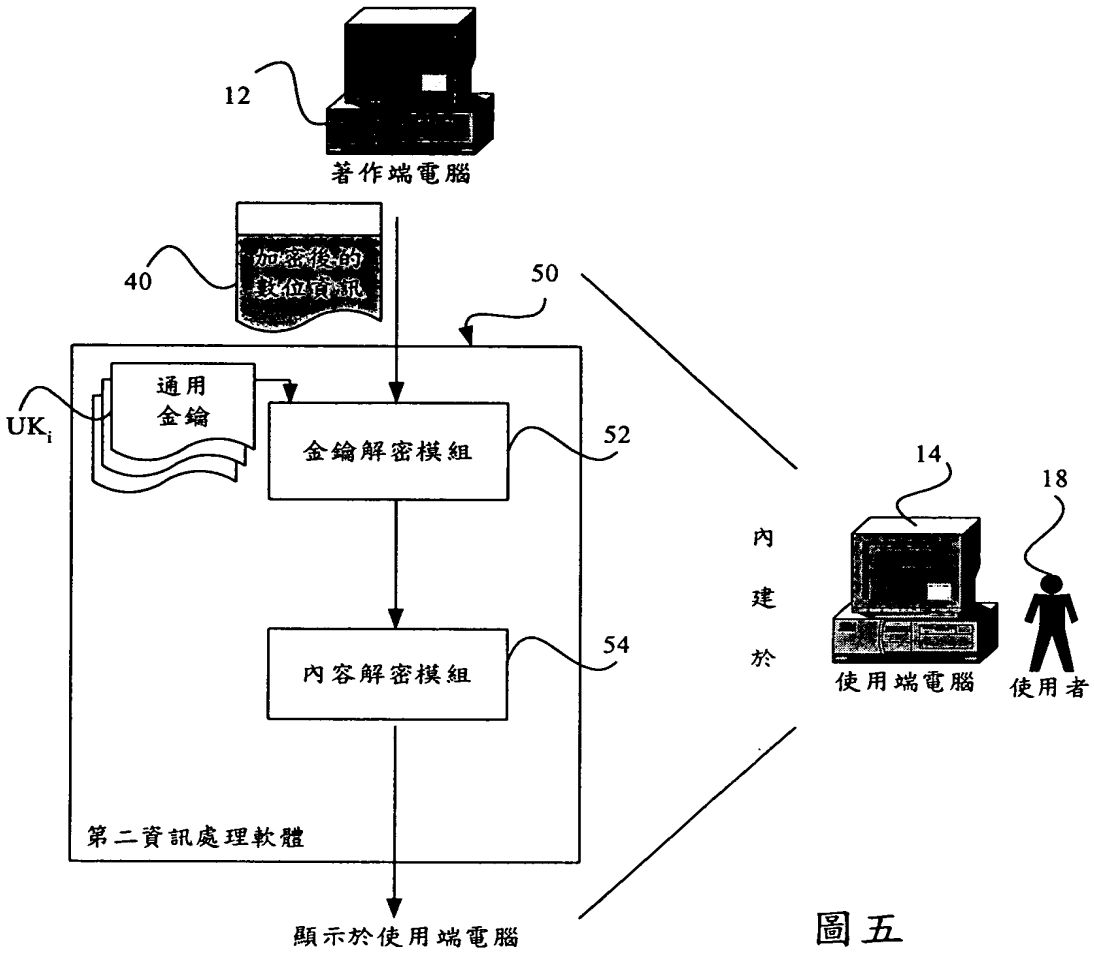
圖三

圖式


接收內容金鑰
S30
加密數位資訊
S31
選擇一通用金鑰
S32
加密內容金鑰
S33
製作標頭檔
S34
將標頭檔附加於
加密後的數位資訊中
S38

圖四

圖式

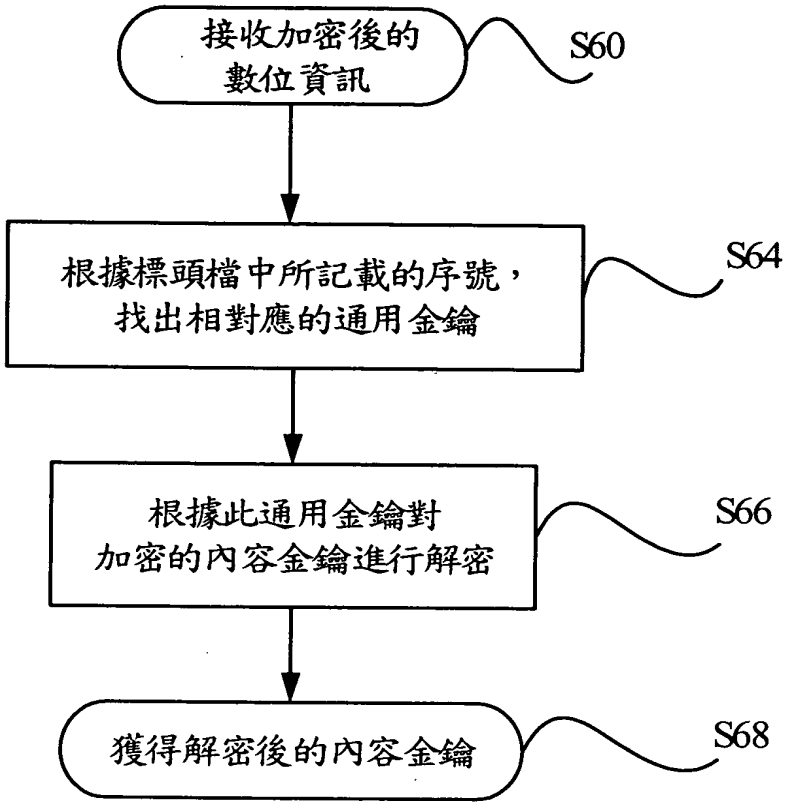

12
著作端電腦
40
加密後的數位資訊
50
通用金鑰
UK_i
金鑰解密模組
52
內容解密模組
54
第二資訊處理軟體
顯示於使用端電腦
內建於
14
使用端電腦
18
使用者

圖五

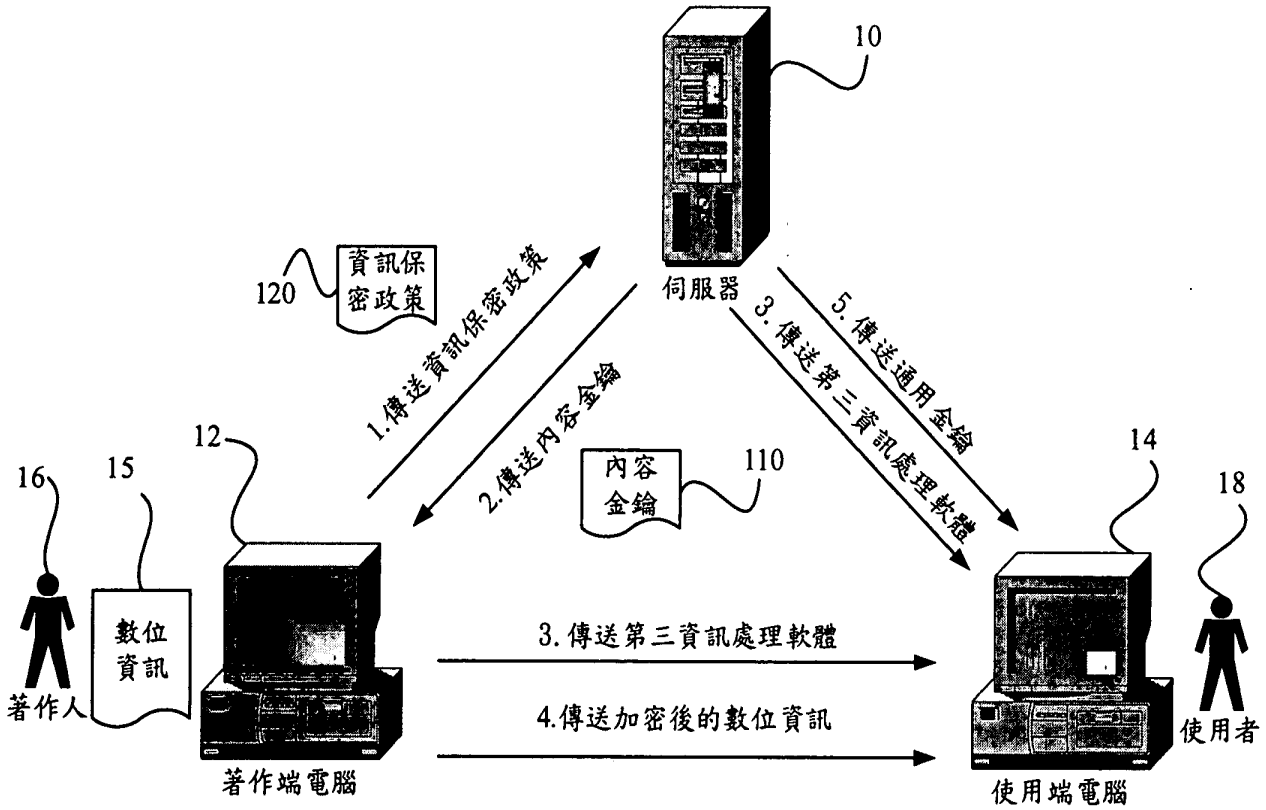
圖式

內容金鑰
110
48
數位資訊
46
44
序號
資訊保密政策
標頭檔
120
42
加密後的內容金鑰
48
數位資訊
46
44
序號
資訊保密政策
標頭檔
120
42
加密後的內容金鑰
48
數位資訊
40

圖六


接收加密後的
數位資訊
S60
根據標頭檔中所記載的序號，
找出相對應的通用金鑰
S64
根據此通用金鑰對
加密的內容金鑰進行解密
S66
獲得解密後的內容金鑰
S68

圖七


10
伺服器
120
資訊保密政策
1.傳送資訊保密政策
2.傳送內容金鑰
內容金鑰
110
3.傳送第三資訊處理軟體
5.傳送通用金鑰
12
16
15
14
18
數位資訊
著作人
3.傳送第三資訊處理軟體
4.傳送加密後的數位資訊
使用者
著作端電腦
使用端電腦

圖八

圖式